UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/811,030	03/26/2004	Jan Hofmeyr	MS1-2018US	9067

22801 7590 02/09/2009

LEE & HAYES, PLLC
601 W. RIVERSIDE AVENUE
SUITE 1400
SPOKANE, WA 99201

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
02/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/811,030	HOFMEYR ET AL.	
	Examiner	Art Unit	
	BENJAMIN E. LANIER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,10-18 and 20-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,10-18 and 20-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/13/2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 17 December 2008 amends claims 1, 14-15, 17, 22, 29-32, and 39. Claim 19 is cancelled. Applicant's amendment has been fully considered and entered.

Response to Arguments

2. Applicant argues, "Candelore nevertheless does not disclose that its PSI 'includes a decryption key for decrypting the encrypted portions,' as recited in Claim 1." This argument is not persuasive because Candelore discloses that the PMT PSI information includes ECMs for the content (Col. 11, lines 63-67 & Col. 12, lines 50-57). ECMs include control words that are used to decrypt the encrypted content (Col. 7, lines 17-19).

3. Applicant points to Figure 1 and corresponding paragraphs of Candelore to suggest that the 'encryption keys are included in additional packets,' however Applicant has failed to realize that the relied upon portion is describing "Prior Art" systems (see Figure 1 which identifies the figure as Prior Art). Therefore, the citations relied upon by Applicant are not related to the actual system of Candelore.

4. Applicant argues, "Candelore also does not disclose, 'generating a multiplex-compliant encryption method packet for each PES header,' as recited in Claim 1." This argument is not persuasive because it is clear that Candelore includes different PSI information for each elementary stream (Col. 7, lines 43-67), which includes a PES header.

5. Applicant argues, "Sparrell cannot be combined with Candelore to disclose, teach, or fairly suggest the above recited element of Claim 1…Sparrell does not disclose PSI information, as 'PSI information' is only disclosed in Candelore." This information is not persuasive because

Applicant is referring to a mere typographical error, and has failed to show why the references cannot be combined.

6. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

7. Applicant's remaining arguments mirror the above, and have been fully addressed.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

10. Claims 1-8, 10-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sparrell, U.S. Patent No. 7,231,516, in view of Candelore, U.S. Patent No. 7,124,303. Referring to claims 1, 8, 12, 13, 16, 22-26, 28, 35, 37, 39, Sparrell discloses an MPEG-2 data stream encryption system wherein program elementary streams are encrypted by encrypting only the

payload data leaving the higher level headers (i.e. PES/frame headers) unencrypted (Col. 10, lines 23-33), which meets the limitation of analyzing a transport stream that includes one or more header portions and one or more corresponding payload portions, each of the header portions includes packetized elementary stream (PES) header and a frame header, wherein each of the header portions enables the processing of the one or more corresponding payload portions based on the PES header, preparing the transport stream for a data extraction by encrypting at least some of the payload portions, while leaving the one or more corresponding header portions unencrypted at all times, encrypting at least some of the payload portions that comprise payload data packets, the payload portions include packets of PES payload data, and wherein preparing the transport stream for the data extraction includes common scrambling at least some of the packets of PES payload data, leave unencrypted data packets having at least a portion of the PES header, leave unencrypted bytes of data required for processing the transport stream, leave unencrypted a threshold amount of data beyond packet header data that is relevant for the processing, encrypt at least some of the payload portions that comprise payload data packets, dynamically determine that a threshold incursion into one payload portion is to pass unencrypted in order to process the transport stream without removing the encryption from other portions of the transport stream. Sparrell does not disclose that payload portions are selectively encrypted. Candelore discloses a partial encryption system for transport streams wherein the cable system headend analyzes the streams to determine which packets should be encrypted (Col. 13, lines 27-33) based upon a desired balance of bandwidth usage and security against hackers (Col. 10, lines 11-14). Program specific information (PSI) for a stream includes information that identifies the encrypted packets (Col. 11, line 60- Col. 12, line 31), and is included within a packet that is

multiplexed into the stream (Col. 11, lines 45-50), which meets the limitation of generating a multiplex-compliant encryption method packet for each PES header, each multiplex-compliant encryption method packet at least identifies encrypted portions of the transport stream, inserting the multiplex-compliant encryption method packet into the transport stream, delivering the multiplex-compliant encryption method packet via a private table. PMT PSI information includes ECMs for the content (Col. 11, lines 63-67 & Col. 12, lines 50-57). ECMs include control words that are used to decrypt the encrypted content (Col. 7, lines 17-19), which meets the limitation of each multiplex-compliant encryption method packet includes a decryption key for decrypting the encrypted portions. It would have been obvious to one of ordinary skill in the art at the time the invention was made to selectively encrypt the payload portions of Sparrell in order to operate the system with a desired balance of bandwidth usage and security as taught in Candelore (Col. 10, lines 14-16).

Referring to claims 2-7, 36, 38, 40, Sparrell discloses an MPEG-2 data stream encryption system wherein program elementary streams are encrypted by encrypting only the payload data leaving the higher level headers (i.e. PES headers) unencrypted (Col. 10, lines 23-33). Sparrell does not disclose that payload portions are selectively encrypted. Candelore discloses a partial encryption system for transport streams wherein the cable system headend analyzes the streams to determine which packets should be encrypted (Col. 13, lines 27-33) based upon a desired balance of bandwidth usage and security against hackers (Col. 10, lines 11-14), which meets the limitation of analyzing the transport stream includes determining which of the one or more payload portions of the transport stream are to pass unencrypted, determining which of the one or more payload portions of the transport stream are to pass unencrypted is executed based on a

statistical analysis, dynamically, determining which of the one or more payload portions of the transport stream are to pass unencrypted includes determining a permissible incursion beyond a header portion into a corresponding payload portion to gather data for the data extraction, detecting a data packet containing at least a portion of a PES header, detecting whether each of the payload portions is in the same data packet as one of the one or more header portions, determine that data arbitrarily disposed throughout PES payload data are to pass unencrypted. It would have been obvious to one of ordinary skill in the art at the time the invention was made to selectively encrypt the payload portions of Sparrell in order to operate the system with a desired balance of bandwidth usage and security as taught in Candelore (Col. 10, lines 14-16).

Referring to claim 10, Sparrell discloses that the frame headers are also left unencrypted (Col. 10, lines 33-36), which meets the limitation of the one or more header portions and the one or more payload portions include data packets, and wherein preparing the transport stream fro the data extraction further includes leaving a data packet containing at least a portion of a frame header unencrypted.

Referring to claim 11, Sparrell discloses that the encrypted transport stream is indexed for trick play mode playback (Col. 10, line 64 – Col. 11, line 51), which meets the limitation of the data extraction includes bypassing encrypted portions of the transport stream to implement one of demultiplexing and indexing the transport stream for at least one of trick modes and thumbnail extraction.

Referring to claims 14, 29, Candelore discloses that the ECMs can be specific to particular encryption algorithms (Col. 26, lines 1-3), which meets the limitation of the multiplex-compliant encryption method packet further identifies an encryption algorithm used in preparing

the transport stream for the data extraction. It would have been obvious to one of ordinary skill in the art at the time the invention was made to selectively encrypt the payload portions of Sparrell in order to operate the system with a desired balance of bandwidth usage and security as taught in Candelore (Col. 10, lines 14-16).

Referring to claims 15, 30, Candelore discloses a partial encryption system for transport streams wherein the cable system headend analyzes the streams to determine which packets should be encrypted (Col. 13, lines 27-33) based upon a desired balance of bandwidth usage and security against hackers (Col. 10, lines 11-14). Program specific information (PSI) for a stream includes information that identifies the encrypted packets (Col. 11, line 60- Col. 12, line 31), and is included within a packet that is multiplexed into the stream (Col. 11, lines 45-50), which meets the limitation of which meets the limitation of the multiplex-complaint encryption method packet further identifies an unencrypted portion of the transport stream, a location of the encrypted portion of the transport stream, and a process corresponding to the unencrypted portion of the transport stream. It would have been obvious to one of ordinary skill in the art at the time the invention was made to selectively encrypt the payload portions of Sparrell in order to operate the system with a desired balance of bandwidth usage and security as taught in Candelore (Col. 10, lines 14-16).

Referring to claims 17, 31, Sparrell discloses an MPEG-2 data stream encryption system wherein program elementary streams are encrypted by encrypting only the payload data leaving the higher level headers (i.e. PES/frame headers) unencrypted (Col. 10, lines 23-33), which meets the limitation of receiving a partially encrypted transport stream that includes one or more header portions, each of the one or more header portions being unencrypted at all times and

including at least one of a packetized elementary stream (PES) header and frame header, and one or more encrypted payload portions, wherein each of the unencrypted header portions enables the processing of the one or more corresponding encrypted payload portions based on at least one of the PES header and the frame header. Leaving the frame headers unencrypted allows for determination of where the I-frames are in the video stream and only transmit the encrypted I-frames across the network, which meets the limitation of extracting data from the transport stream in a manner that bypasses the one or more encrypted payload portions of the transport stream. Sparrell does not disclose that payload portions are selectively encrypted. Candelore discloses a partial encryption system for transport streams wherein the cable system headend analyzes the streams to determine which packets should be encrypted (Col. 13, lines 27-33) based upon a desired balance of bandwidth usage and security against hackers (Col. 10, lines 11-14). Program specific information (PSI) for a stream includes information that identifies the encrypted packets (Col. 11, line 60- Col. 12, line 31), and is included within a packet that is multiplexed into the stream (Col. 11, lines 45-50), which meets the limitation of generating a multiplex-compliant encryption method packet that at least identifies encrypted portions of the transport stream, inserting the multiplex-compliant encryption method packet into the transport stream, delivering the multiplex-compliant encryption method packet via a private table. PMT PSI information includes ECMs for the content (Col. 11, lines 63-67 & Col. 12, lines 50-57). ECMs include control words that are used to decrypt the encrypted content (Col. 7, lines 17-19), which meets the limitation of each multiplex-compliant encryption method packet includes a decryption key for decrypting the encrypted portions. It would have been obvious to one of ordinary skill in the art at the time the invention was made to selectively encrypt the payload

portions of Sparrell in order to operate the system with a desired balance of bandwidth usage and security as taught in Candelore (Col. 10, lines 14-16).

Referring to claims 18, 32, Candelore discloses that PSI information include the keys used to decrypt the stream (Col. 8, lines 38-67), which meets the limitation of receiving the multiplex-compliant encryption method packet corresponding to the transport stream, and decrypting encrypted payload portions of the transport stream using a decryption/encryption key, the decryption key is included in the encryption method packet.

Referring to claims 20, 33, Sparrell discloses leaving the frame headers unencrypted allows for determination of where the I-frames are in the video stream and only transmit the encrypted I-frames across the network, which meets the limitation of demultiplexing the transport stream based on unencrypted header portions of the transport stream.

Referring to claims 21, 34, Sparrell discloses that the index information identifies which segments of the stream have been encrypted and with what key (Col. 7, lines 61-65), which meets the limitation of indexing payload data contained in the transport stream based on unencrypted header portions of the transport stream.

Referring to claim 27, Sparrell discloses that the stream can be encrypted using AES (Col. 12, lines 42-43), which meets the limitation of encrypt portions of the transport stream applies an advanced encryption standard (AES) counter (CTR) mode cipher.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 7:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432